Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

Nederlands Schema
voor Certificatie op het
gebied van IT-Beveiliging
(NSCIB)

NSCIB Scheme Instruction 00

International Supporting Documents

Approved.......................................

Technical Manager NSCIB

Instruction	00
Report title	International Supporting Documents
Date of issue	November 23, 2023
Version	1.13
Distribution	Public
Filename	NSI_00_International_Supporting_Documents_v1.13.docx

TRUSTCB®
TRUST AND VERIFY

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

1 Purpose of this document

To provide an overview of all international supporting documents that are to be used in CC evaluations where applicable.

2 Background and application

This instruction provides the formal framework to embed all supporting documents that are issued under the responsibility of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) into the NSCIB processes. This instruction will regularly be updated when new or updated international supporting documents are available.

The referenced international supporting documents are in effect immediately and need to be applied when a product involving the particular technology is being evaluated or the subject of the document is of general use in all CC evaluations. The version and date of issue of this instruction needs to be referenced in the appropriate section of annex B of the Application Form, thereby making it clear which versions of the international supporting documents need to be applied for the specific CC evaluation.

3 International supporting documents

Note that for some of the documents listed below there is both a CCRA/CC supporting document and a JIL document available. These are normally equivalent whereas the JIL document takes precedence and needs to be applied and referenced in the Evaluation Technical Report (ETR) when the certificate falls under the SOG-IS MRA recognition.

Documents listed in grey-italics are considered to be guidance and contain non-mandatory general advice.

3.1 CCRA/CC supporting documents

The following documents are CCRA/CC supporting documents that are available on the Common Criteria Portal website[1].

Document reference	Description
[CCDB-2006-04-004]	ST sanitising for publication, April 2006.
[CCDB-2007-11-001]	*Site Certification, Version 1.0, October 2007.*
[CCDB-2012-04-005]	*Collection of Developer Evidence, Version 1.5, April 2012.*
[CCDB-011-v2.2-2021-Sep-30]	Assurance Continuity: CCRA Requirements, Maintained by CCDB, Version 2.2, 3 September 2021.

3.2 SOG-IS MRA/JIL documents

The following documents are issued by the SOG-IS Crypto Work Group or Joint Interpretation Work Group (JIWG). They can be found in the same order on the SOGIS website[2] with the exception of the sensitive documents which are available through the CB.

Document reference	Description
[JIL-AC]	Assurance Continuity, Version 1.1, June 2023.
[JIL-VD]	JIL-Coordinated-Vulnerability-Disclosure and handling processes, Version 1.0, October 2020. For trial use.
[JIL-CV]	SOG-IS certificate validity, Version1.0, January 2020.
[AgreedCrypto]	*SOG-IS Agreed Cryptographic Mechanisms, Version 1.3, February 2023.*

[1] See https://www.commoncriteriaportal.org/cc/

[2] See http://sogis.eu/uk/detail_operation_en.html and http://sogis.eu/uk/supporting_doc_en.html and https://www.sogis.eu/uk/pp_en.html

[JIL-Collect]	*Collection of Developer Evidence, Version 1.5, January 2012.*
[JIL-EMP]	*Evaluation methodology for product series, Version 1.0, April 2017.*
[JIL-MSSR]	Minimum Site Security Requirements, Version 3.0, February 2020. [3]
[JIL-MSSRcl]	*Minimum Site Security Requirements Checklist, Version 3.0, February 2020.*
[JIL-AAPS]	Application of Attack Potential to Smartcards, Version 3.2, November 2022.
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution).
[JIL-IC]	The Application of CC to Integrated Circuits, Version 3.0, February 2009.
[JIL-COMP]	Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.
[JIL-ETRfC]	*ETR for composition evaluation template, version 1.1, August 2015.*
[JIL-SC]	*Guidance for smartcard evaluation, Version 2.0, February 2010.*
[JIL-ARC]	Security Architecture requirements (ADV_ARC) for smart cards, and similar devices extended to Secure Sub-Systems in SoC, Version 2.1, July 2021.
[JIL-ARCappx]	Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub-Systems in SoC Appendix 1 *Version 2.1, July 2021.*
[JIL-VA-SoC]	*Guidance for Vulnerability Analysis and Penetration Testing of a Secure Sub-System within a System-on-Chip, version 2.0 Release 4, June 2021(sensitive with controlled distribution).*
[JIL-OPEN]	Certification of “open” smart card products, Version 1.1, 4 February 2013. For trial use.
[JIL-POST]	*Security requirements for post-delivery code loading, Version 1.0, February 2016.*
[JIL-ITSEF-SC]	Minimum ITSEF Requirements for Security Evaluations of Smart Cards and similar devices, Version 2.1, February 2020.
[JIL-AC]	*Assurance Continuity – Practical cases for Smart Cards and similar devices, Version 1.0, November 2017.*
[JIL-SWIP]	*Management of Code Disclosure and Software IP Reuse, Version 1.2, November 2017.*
[JIL-STAR]	*Site Technical Audit Report Template, Version 1.0, February 2018.*

[3] *Guidance: the objective of guidance documents is for developers, ITSEFS and certification body's to improve the evaluation and certification process. Guidance documents may contain background material to aid the understanding of the evaluation approach or any other information and hold no obligations for any of the involved actors.*

Mandatory: supporting documents of the type 'Mandatory' contain a consistent set of interpretations that specify the use of the criteria and methodology within a particular field or domain of technology and shall be used where relevant. These documents contain the elements necessary for mutual recognition of certificates for such technologies. The Evaluation Technical Report and the Certification Report shall identify which mandatory supporting documents have been used (incl. version).

Trial use: before a supporting document is approved as mandatory, a trial use phase will take place. The objective of the trial use phase is to gain experience in the application of the requirements of a mandatory supporting document in the context of a product evaluation. The application of the documents for trial use is mandatory for the certification under the SOGIS-MRA for all products within a particular field or domain of technology.

During the trial phase period it is expected that additional support from the CB in charge of the certification will be provided to interpret the trial-use document on case by case basis when problems with its applications arise. The interpretations that have been identified during the trial use phase will be fed back to their editors in order to improve the documents in a next version. This is expected from ITSEFS (JIWG WG's). The CB is expected to feed this back to NLCSA (JIWG).

[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.1, November 2023.
[JIL-AMHD]	Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution).
[JIL-ITSEF-HD]	Minimum ITSEF Requirements for Security Evaluations of Hardware Devices with Security Boxes, Version 1.1, August 2020.
[JIL-HSMPP]	Guidance for HW assessment in EN 419221-5 (HSM PP) v1.0, May 2021.

3.3 Evaluation specific methods

The following documents are issued by the BSI. They can be found on their website[4] with the exception of the sensitive documents which are available through the CB.

Document reference	Description
[AIS 20/31]	Functionality classes and evaluation methodology for deterministic/physical random number generators, version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik
[AIS 34]	Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6, version 3, 03.09.2009, Bundesamt für Sicherheit in der Informationstechnik
[AIS 46]	Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, version 3, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik: • Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations • Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations • Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices

[4] BSI: www.bsi.bund.de